

抗矿池集中化的共识机制研究

【 区块链； 共识机制； 矿池集中化； POW； POS； POWS 】

- 指导老师：李志淮 教授
- 答辩人：杨超智

目录

CONTENTS

- 01 选题背景
- 02 问题分析
- 03 POWS共识机制设计
- 04 实验与分析
- 05 总结与展望
- 06 攻读学位期间公开发表论文

01

选题背景

区块链技术

区块链的本质是一个去中心化的分布式总账本

具有**去中心化**、**去信任**、**集体维护**、**不可更改**的特点

使用区块链的原因

传统的集中模式存在**不可靠**、**不可信**的问题

区块链的发展前景

2018年2月，**人民日报**经济周刊发布整版专题报道《三问区块链》，
《**抓住区块链这个机遇**》以及《**做数字经济领跑者**》，
以积极的态度肯定了区块链技术具有突破性意义。

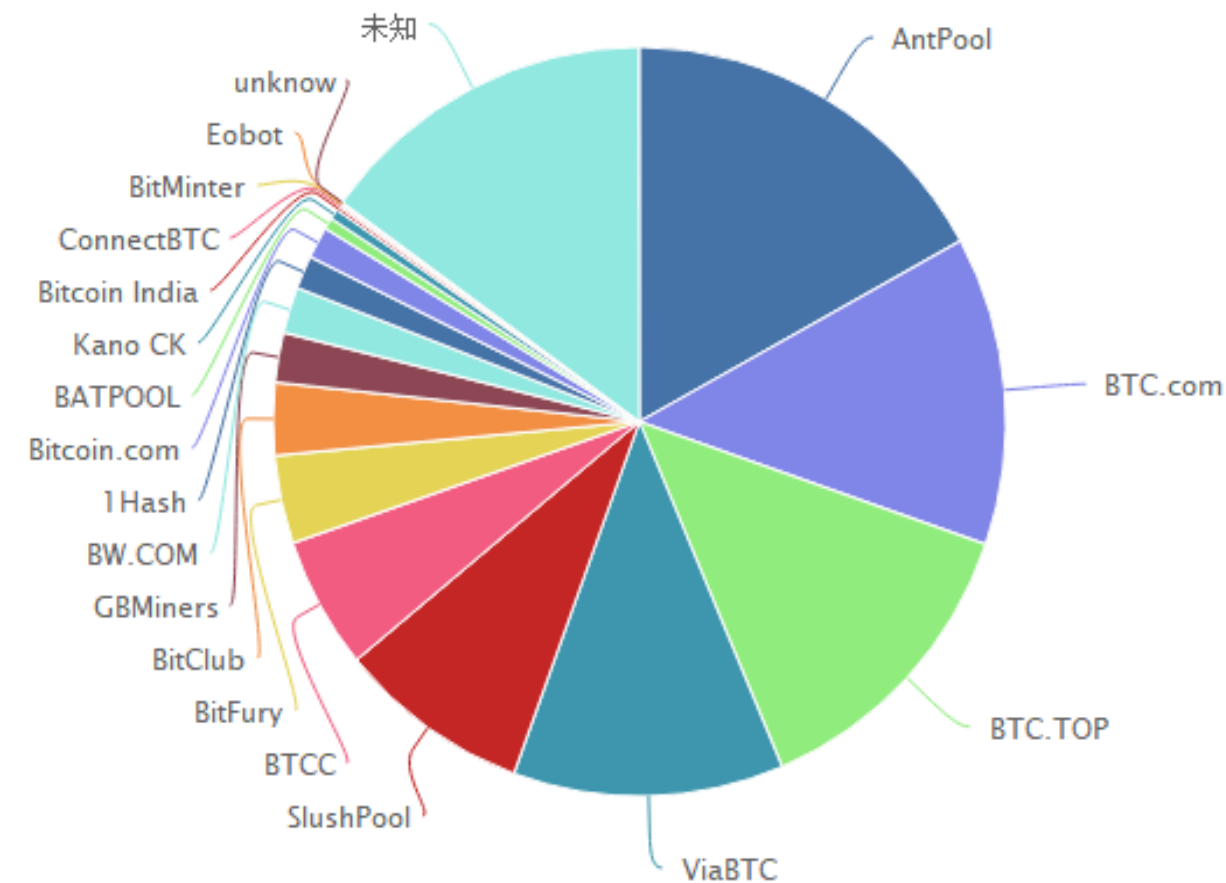


- **区块链1.0**
以比特币、莱特币等为代表的数字货币交易系统
- **区块链2.0**
以以太坊、量子链、NEO为代表的**智能合约**平台

02

问题分析

——“去中心化”的异化



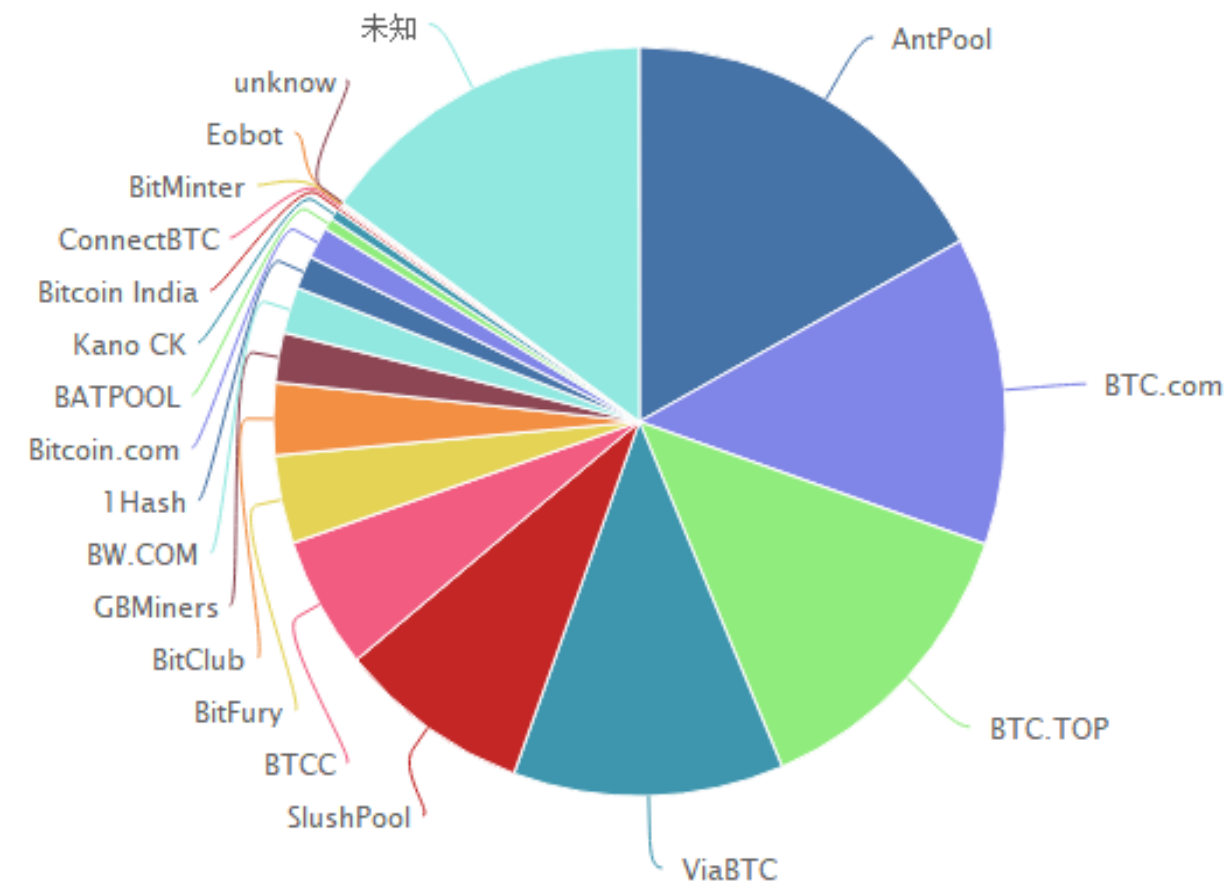
比特币算力分布图

POW矿池导致异化

比特币使用的共识机制是**POW**
(Proof-of-Work) 工作量证明机制

POW共识机制需要耗费大量的算力进行哈希计算，通过工作量来证明新区块的铸造权，这个过程被称为**挖矿**

利益集团囤积算力组建**矿池**，违背了去中心化的初衷



比特币算力分布图

POW矿池导致异化

比特币算力被大大小小十几家矿池所占据

比特币其实已经类似于由十几个矿池组成的区块链矿池**联盟链**

各大矿池垄断了比特币算力后，可以随意进行比特币**分叉 (IFO)**

- **造成矿池集中化的主要原因**
- 矿池集中化的问题广泛存在于POW和POS（Proof-of-Stake）权益证明机制机制中
矿池集中化不仅会造成一定效应的中心化，还会使区块链网络随时面临着遭受**51%攻击**的风险。
- 矿池组织依靠庞大的财力和行业影响力，购置大量的先进挖矿设备和币，囤积算力和币龄。利用现有共识机制的缺陷提升区块链网络的整体挖矿难度，使得普通矿工节点与矿池节点形成巨大的出块效率差距。巨大的出块效率差距，驱动大量普通节点加入矿池，从而达到矿池集中化。

其中使普通矿工节点与矿池节点形成**巨大的出块效率差距**，用实实在在的**利益驱动普通节点加入矿池**是造成矿池集中化的**最重要原因**。

- 主流共识机制中的矿池集中化问题及主要解决方法

	POW	POS	DPOS
解决方法	无	放弃算力，引入币龄	放弃算力和币龄， 引入股东代表机制
弊端	算力集中化，IFO	币龄集中化	代表垄断

03

POWS共识机制 设计

- POWS共识机制

为了解决矿池集中化的问题，为了**降低**普通矿工节点与矿池节点的**出块效率差距**，**降低**矿池对普通节点**利益驱动**，秉承着POW+POS的混合模式思想，本文设计了POWS (基于权益调节的工作量证明机制，Proof-of -Work Adjusted by Stake) 并通过实验进行验证。

POWS共识机制

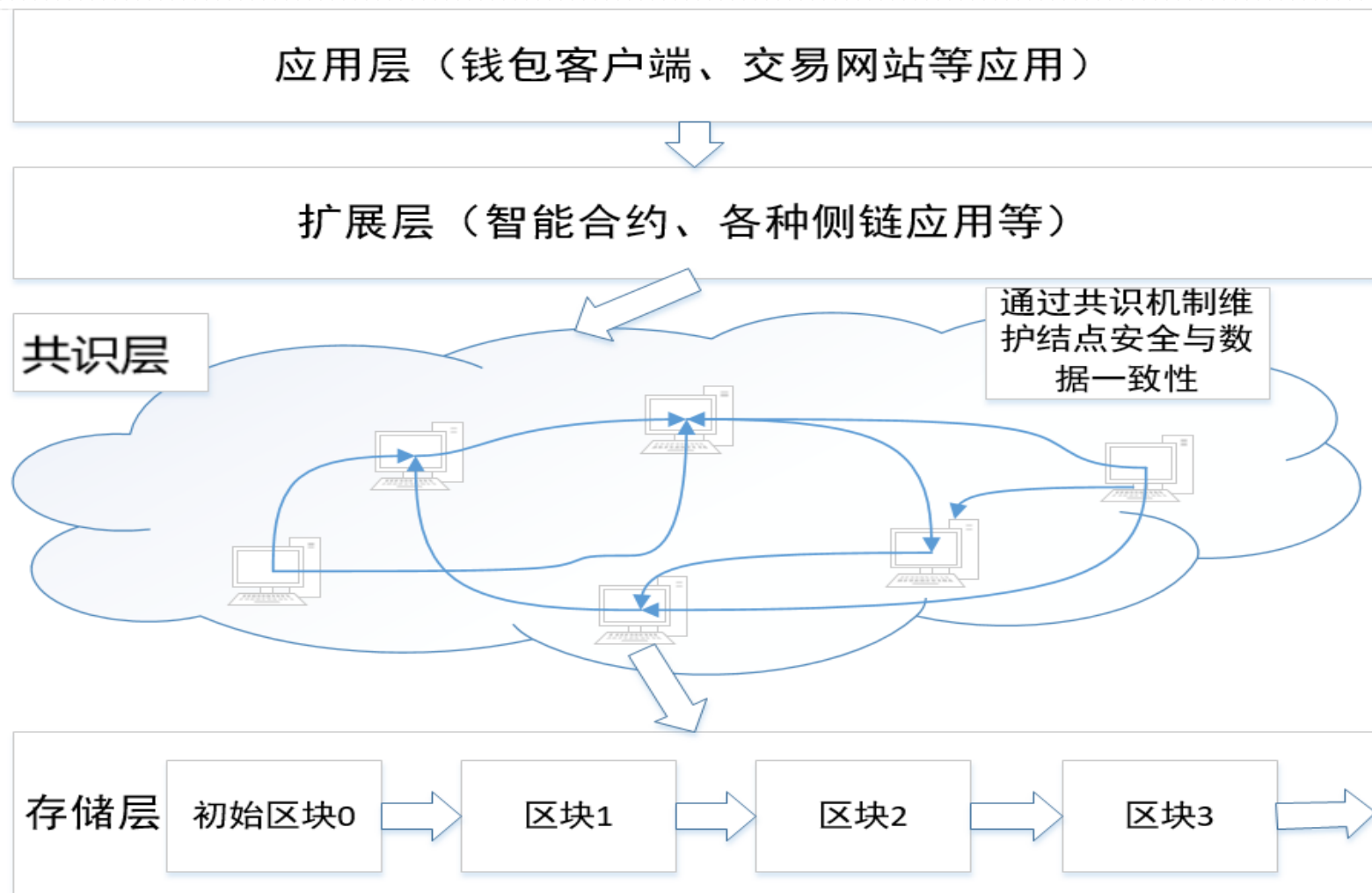
矿池算力（币龄）来源	矿池囤积	普通结点加入矿池贡献
POWS解决方法	引入 币龄调节 不同结点的 挖矿难度 并减弱算力和币龄增大时对出块效率得影响，利用算力和币龄两个因素共同制约矿池	通过调节不同结点的挖矿难度，减小矿池结点和非矿池结点的出块效率差距， 降低 矿池对非矿池结点的 利益驱动

- POWS共识机制

POWS共识机制的核心思想是引入**UTXO总币龄和**的概念用以调节不同结点的挖矿难度，同时依然采用消耗算力的工作量证明方式，通过**算力**和**币龄**两个方面影响产生区块的概率。

$$\text{SumCoinAge} = \sum_{i=0}^n (\text{Value}_i * \text{Input}_i)$$

$$\text{Target} = \sqrt{\text{SumCoinAge}} * \text{coefficient} * 2^{(8 * (\text{exponent} - 3))}$$



P2P节点网络

底层的P2P网络参考BitCoin底层网络

区块链类别

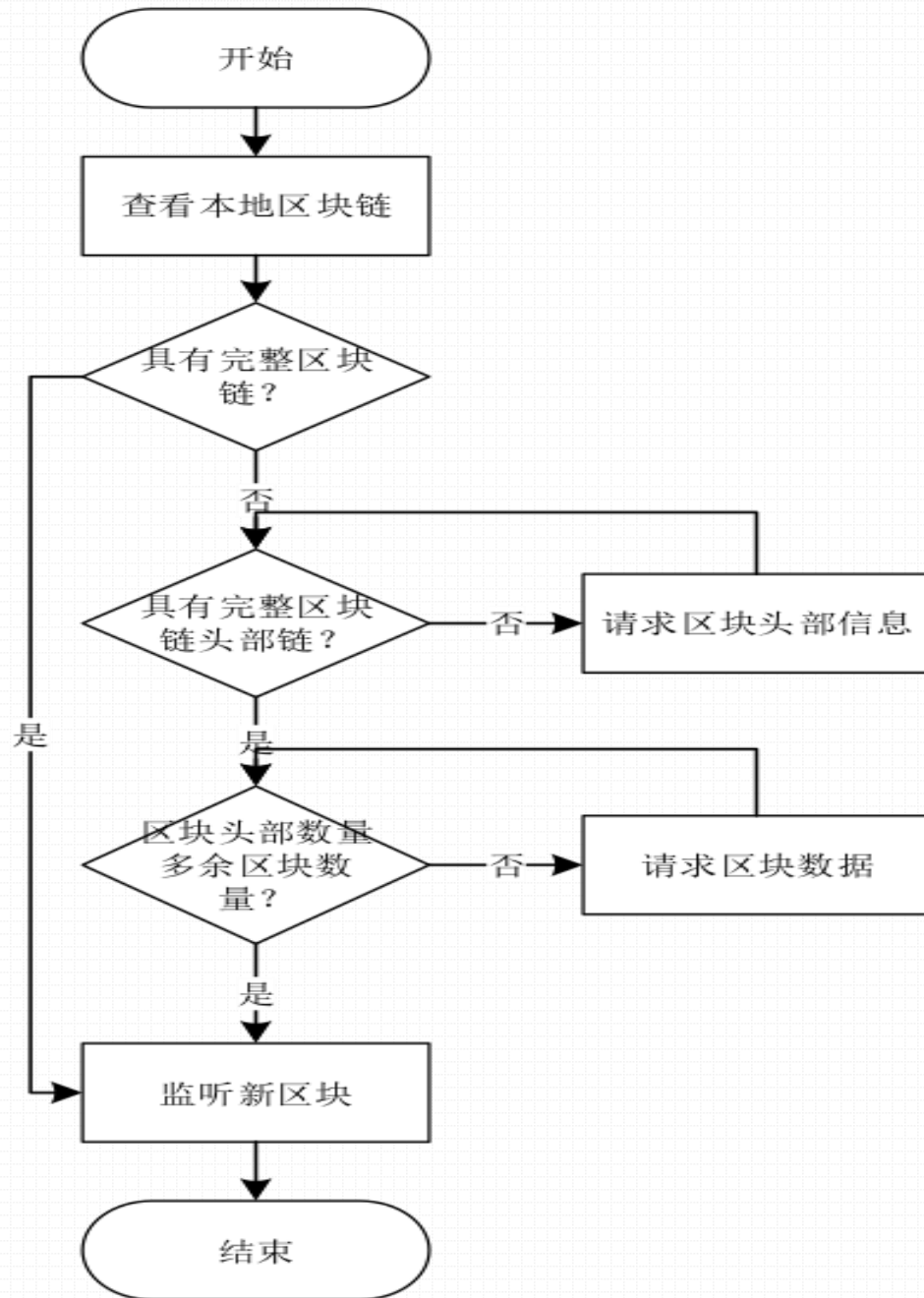
采用**公有链**，结点自由加入

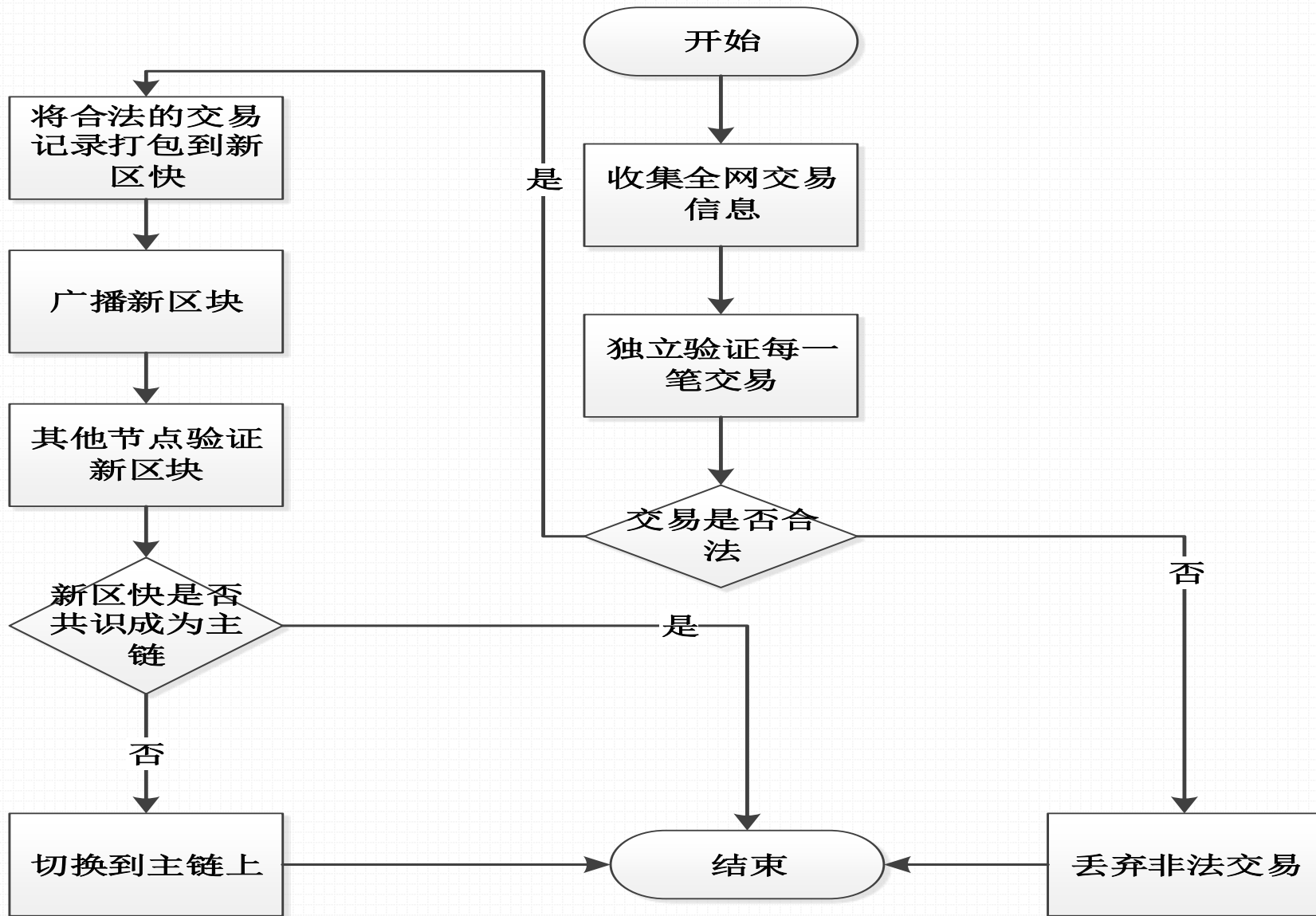
共识机制

本文设计的POWS共识机制，引入**币龄**的概念用以调节不同结点的区块产生**难度**

区块结构

在原有区块结构的基础上修改，添加**总币龄和**的相关部分





04

实验与分析

基本性能实验

1. 平均出块时间对比实验
2. 抗负载对比实验

抗矿池化实验

1. 平均出块效率随算力变化对比实验
2. 平均出块效率随币龄变化对比实验
3. POWS矿池对非矿池节点利益驱动实验

表1 实验硬件环境说明
Tab. 1 Experiment hardware environment description

名称	内存	CPU主频	内核数	数量	硬盘大小	操作系统	内网IP
服务器1号	16GB	Intel Xeon E5620/2.4GHz	4	8	500GB	Ubuntu 16.04	192.168.10.1
服务器2号	16GB	Intel Xeon E5620/2.4GHz	4	8	500GB	Ubuntu 16.04	192.168.10.2
服务器3号	16GB	Intel Xeon E5620/2.4GHz	4	16	500G	Ubuntu 16.04	192.168.10.3
服务器4号	16GB	Intel Xeon E5620/2.4GHz	4	8	1TB	Ubuntu 16.04	192.168.10.4
服务器5号	16GB	Intel Xeon E5620/2.4GHz	4	8	1TB	Ubuntu 16.04	192.168.10.5
服务器6号	16GB	Intel Xeon E5620/2.4GHz	4	8	500G	Ubuntu 16.04	192.168.10.6
服务器7号	16GB	Intel Xeon E5620/2.4GHz	4	8	300G	Ubuntu 16.04	192.168.10.7
服务器8号	16GB	Intel Xeon E5620/2.4GHz	4	8	350G	Ubuntu 16.04	192.168.10.8

```
root@ubuntu:~/bitcoin# bitcoin-cli getinfo
{
  "version": 140200,
  "protocolversion": 70015,
  "walletversion": 130000,
  "balance": 0.00000000,
  "blocks": 1728,
  "timeoffset": 2,
  "connections": 8,
  "proxy": "",
  "difficulty": 1,
  "testnet": false,
  "keypoololdest": 1504493133,
  "keypoolsize": 100,
  "paytxfee": 0.00000000,
  "relayfee": 0.00001000,
  "errors": ""
}
```

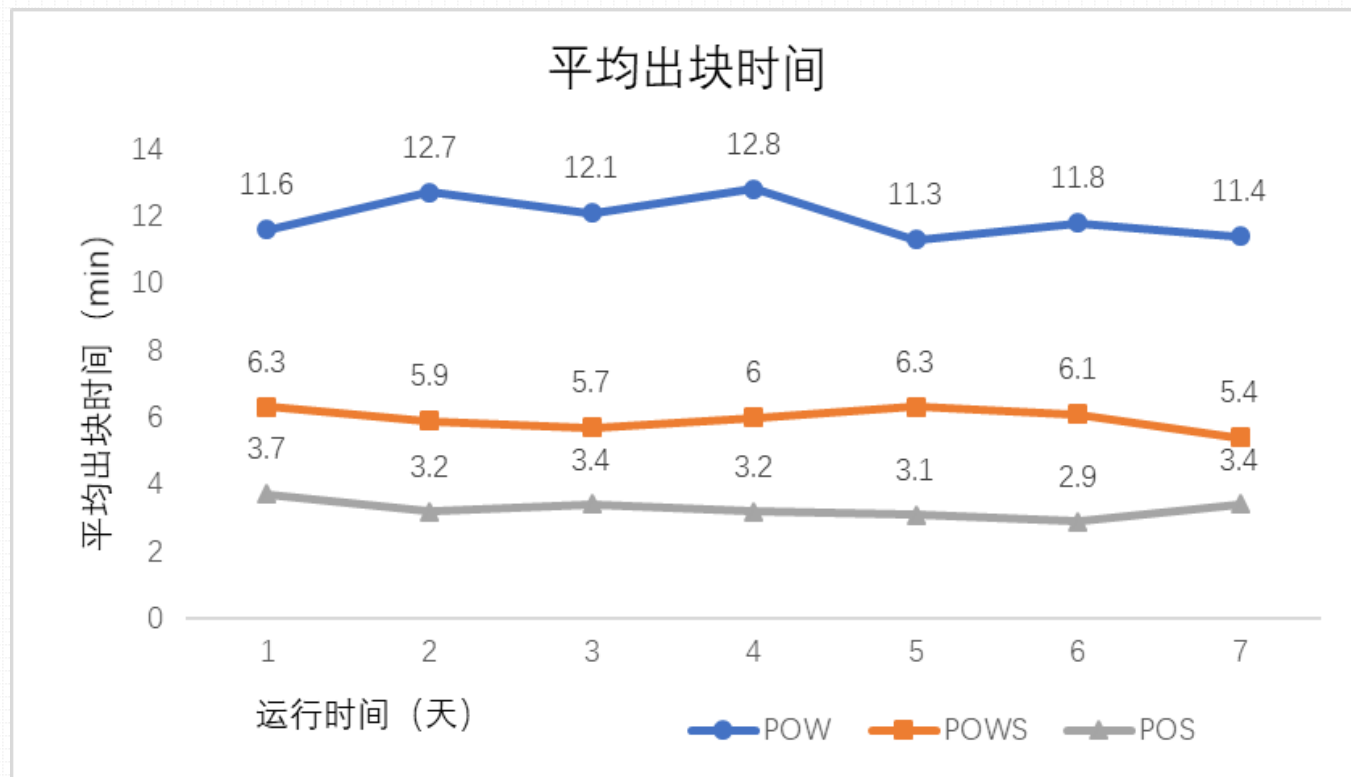
图1 Bitcoin Core版本信息

Fig. 1 Version information of the Bitcoin Core

```
mysql> select * from blockinfo where blockindex>494900;
+-----+-----+-----+-----+
| blockindex | txnum | vin  | vout |
+-----+-----+-----+-----+
| 494901 | 1955 | 4702 | 5647 |
| 494902 | 2098 | 5204 | 6147 |
| 494903 | 2526 | 4790 | 7295 |
| 494904 | 2068 | 5195 | 5682 |
| 494905 | 2243 | 4902 | 6311 |
```

图2 Bitcoin交易数据集信息

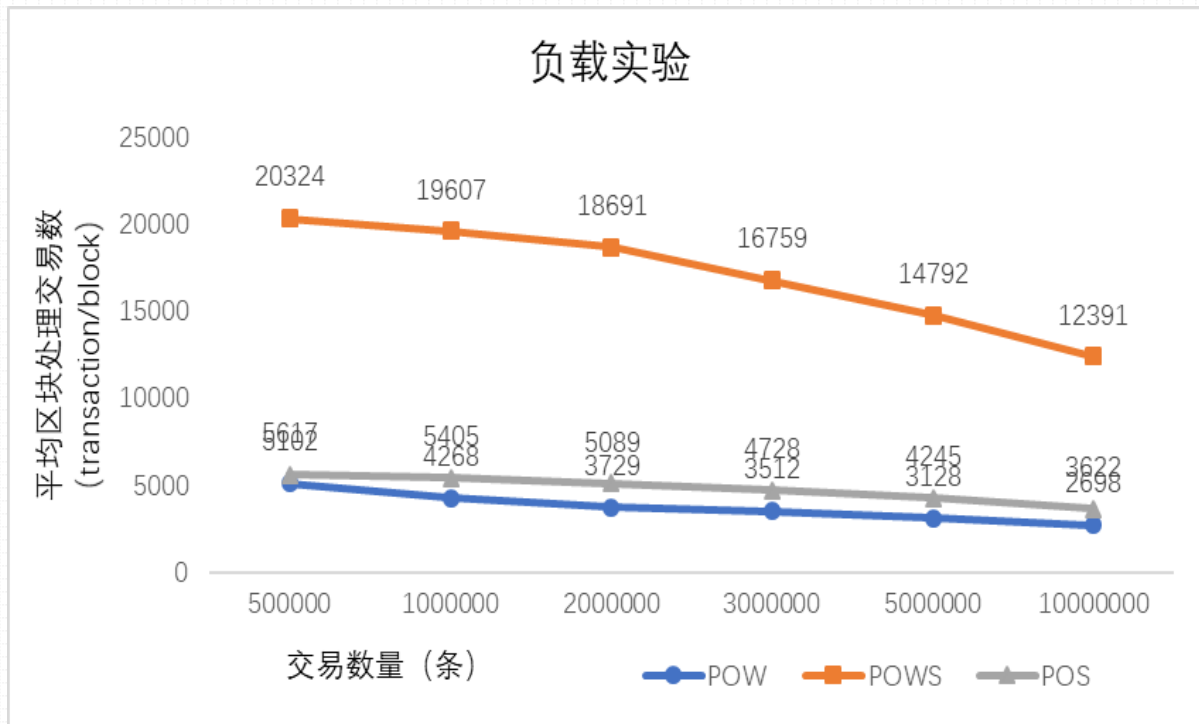
Fig. 2 Bitcoin Transaction data set



POWS共识机制的平均
出块时间快于POW,慢
于POS

图3 平均出块时间

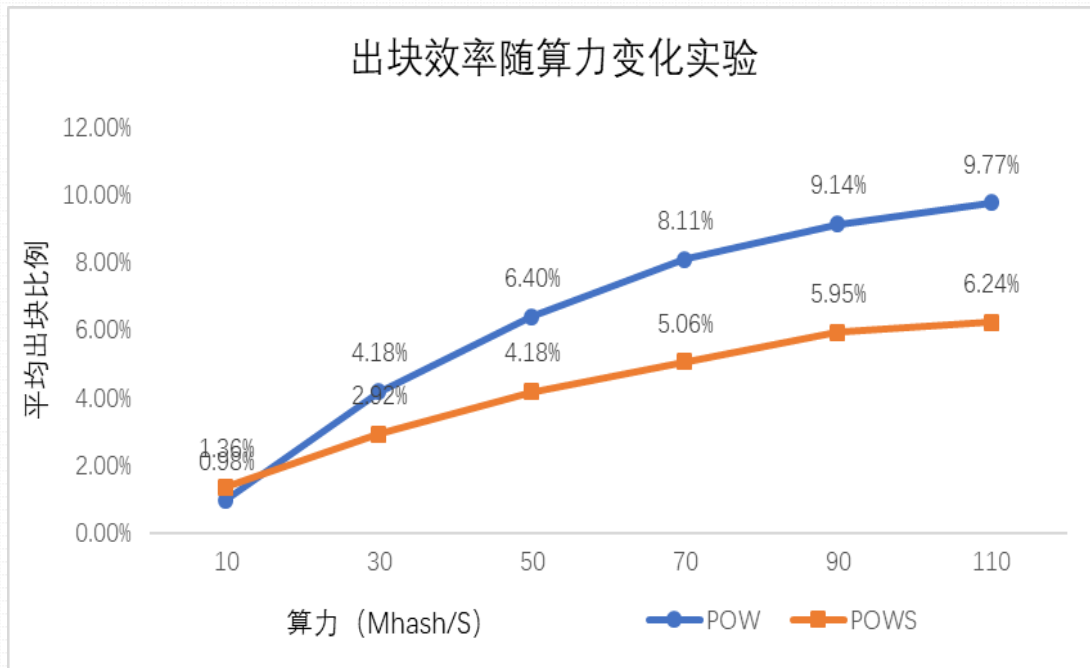
Fig. 3 Average time of make block



POWS共识机制的交易
处理能力优于POW和
POS

图4 负载实验

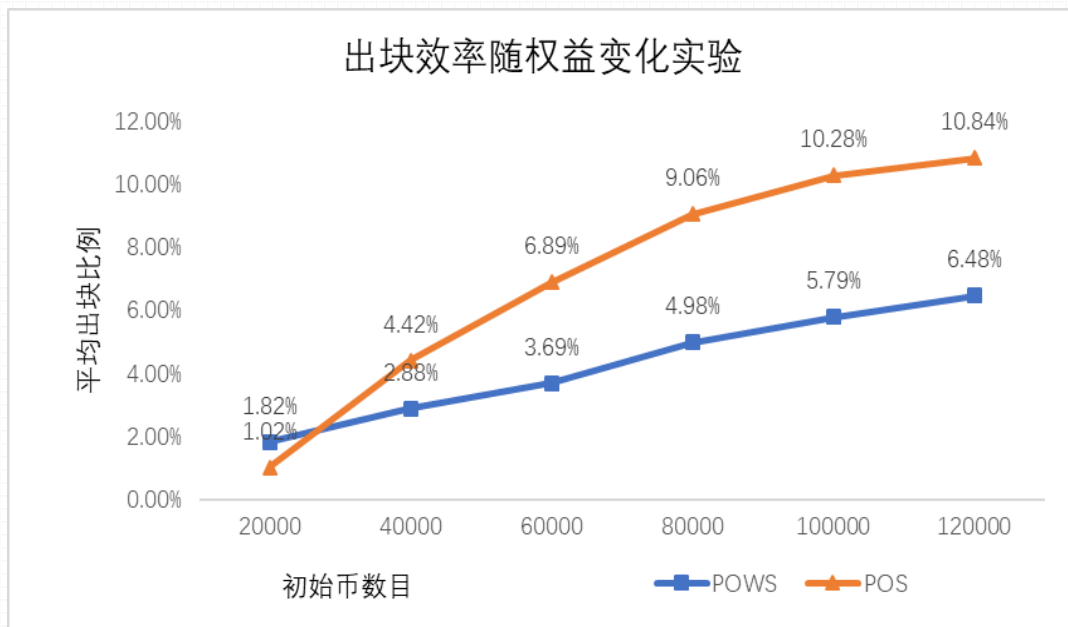
Fig. 4 Load experiment



算力对POWS共识机制
的影响更小

图5 出块效率与算力实验

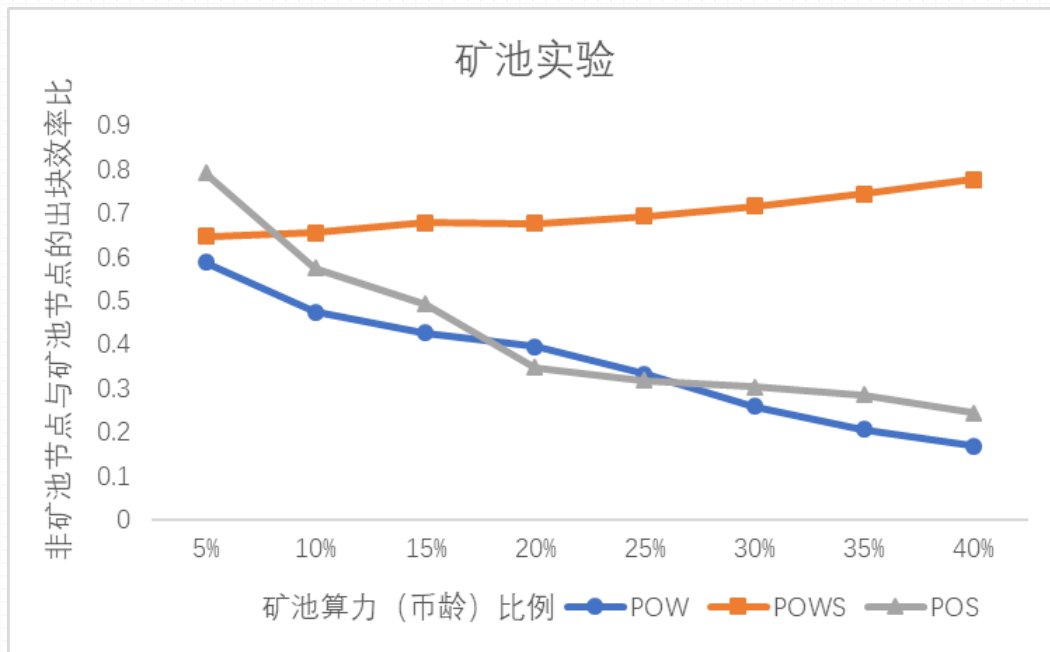
Fig. 5 Block efficiency and calculation of power experiment



币龄（权益）对POWS
共识机制的影响更小

图6 出块效率与权益实验

Fig. 6 Block efficiency and stake experiment



POWS共识机制的普通
节点与矿池节点之间
的平均出块效率差距
比POW和POS 更小

图7 矿池实验

Fig. 7 Mine pool experiment

POWS共识机制**降低**了矿池节点与非矿池节点的**平均出块效率差距**，**降低**矿池对普通节点的**利益驱动**，使得矿池组织难以吸引普通节点加入矿池。

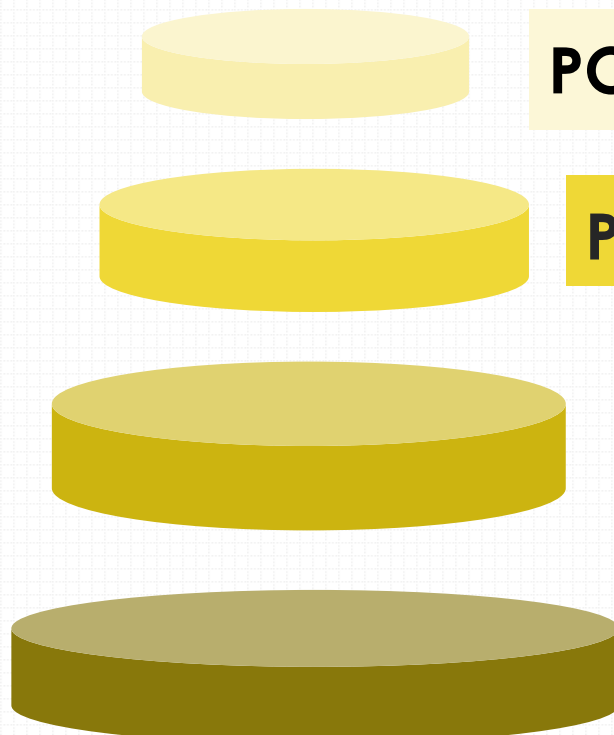
POWS共识机制中，矿池节点和普通节点之间虽然仍有一定的平均出块效率差距，但事实上这些差距也并不会全部兑现且矿池节点相比于普通节点有着很多**弊端**。

矿池中心化挖矿详情**不可信**

矿池中心化管理代币**不可信**

05

总结与展望




POWS共识机制中普通节点与矿池节点的平均出块效率差距更小


POWS共识机制中矿池对非矿池节点的利益驱动更小

POWS共识机制的平均出块效率受算力的影响更小


POWS共识机制的平均出块效率受币龄的影响更小



降低POWS
共识机制的
算力消耗



缩短POWS
区块的生成
时间



改进激励机
制，用以激
励在缺少矿
池情况下普
通矿工节点
参与的积极
性

06

攻读学位期间公
开发表论文

- [1] **Chaozhi Yang**, Tingting Cai, Zhihuai Li. Research on a tunable consistency strategy of the distributed database. International Conference on Information, Cybernetics and Computational Social Systems (ICCSS), 2017, 533-538.
(EI: 20180304657083)

感谢！

THANK YOU!

《抗矿池集中化的共识机制研究》

- 指导老师：李志淮 教授
- 答辩人：杨超智